Cold River - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:19:55 UTC

APT group: Cold River

Names	Cold River *(Lastline)* Nahr el bared *(original place)* Nahr Elbard *(transliteration)* Cobalt Edgewater *(SecureWorks)* TA446 *(Proofpoint)* Seaborgium *(Microsoft)* TAG-53 *(Recorded Future)* BlueCharlie *(Recorded Future)* Blue Callisto *(PWC)* Calisto *(Sekoia)* Star Blizzard *(Microsoft)* UNC4057 *(Mandiant)* IRON FRONTIER *(SecureWorks)* Grey Pro *(?)* Mythic Ursa *(Palo Alto)* Gossamer Bear *(CrowdStrike)*
Country	Russia
Sponsor	State-sponsored, FSB Centre 18: Centre for Information Security (TsIB)
Motivation	Information theft and espionage
First seen	2019
Description	(Lastline) While reviewing some network anomalies, we recently uncovered Cold River, a sophisticated threat actor making malicious use of DNS tunneling for command and control activities. We have been able to decode the raw traffic in command and control, find sophisticated lure documents used in the campaign, connect other previously unknown samples, and associate a number of legitimate organizations whose infrastructure is referenced and used in the campaign. The campaign targets Middle Eastern organizations largely from the Lebanon and United Arab Emirates, though, Indian and Canadian companies with interests in those Middle Eastern countries are also targeted. There are new TTPs used in this attack – for example Agent_Drable is leveraging the Django python framework for

	command and control infrastructure, the technical details of which are outlined later in the blog.	
Observed	Sectors: Defense, NGOs, Think Tanks. Countries: Canada, India, Lebanon, UAE, Ukraine, USA, NATO.	
Tools used	DNSpionage, LOSTKEYS, SPICA.	
Operations performed	Feb 2022	Blue Callisto orbits around US Laboratories in 2022 <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html>
	Mar 2022	COLDRIVER, a Russian-based threat actor sometimes referred to as Calisto, has launched credential phishing campaigns, targeting several US based NGOs and think tanks, the military of a Balkans country, and a Ukraine based defense contractor. However, for the first time, TAG has observed COLDRIVER campaigns targeting the military of multiple Eastern European countries, as well as a NATO Centre of Excellence. <https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe/>
	Apr 2022	COLDRIVER, a Russian-based threat actor sometimes referred to as Callisto, continues to use Gmail accounts to send credential phishing emails to a variety of Google and non-Google accounts. <https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/>
	Jul 2022	Exposing TAG- 53's Credential Harvesting Infrastructure Used for Russia-Aligned Espionage Operations <https://go.recordedfuture.com/hubfs/reports/cta-2022-1205.pdf>
	Aug 2022	Russian hackers targeted U.S. nuclear scientists <https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06/>
	Nov 2022	Russian threat group COLDRIVER expands its targeting of Western officials to include the use of malware <https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/>
	Mar 2023	BlueCharlie, Previously Tracked as TAG 53, Continues to Deploy New Infrastructure in 2023 <https://go.recordedfuture.com/hubfs/reports/cta-2023-0802.pdf>

	Sep 2024	Russian pro-democracy nonprofit investigates alleged data breach by Kremlin-backed hackers <https://therecord.media/free-russia-foundation-data-breach>
	Nov 2024	New Star Blizzard spear-phishing campaign targets WhatsApp accounts <https://www.microsoft.com/en-us/security/blog/2025/01/16/new-star-blizzard-spear-phishing-campaign-targets-whatsapp-accounts/>
	Jan 2025	COLDRIVER Using New Malware To Steal Documents From Western Targets and NGOs <https://cloud.google.com/blog/topics/threat-intelligence/coldriver-steal-documents-western-targets-ngos>
Counter operations	Aug 2022	Disrupting SEABORGIUM's ongoing phishing operations <https://www.microsoft.com/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/>
	Oct 2024	Protecting Democratic Institutions from Cyber Threats <https://blogs.microsoft.com/on-the-issues/2024/10/03/protecting-democratic-institutions-from-cyber-threats/>
Information	<https://www.lastline.com/labsblog/threat-actor-cold-river-network-traffic-analysis-and-a-deep-dive-on-agent-drable/> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format
